



Distinguished representations of non-negative polynomials

Claus Scheiderer

Fachbereich Mathematik und Statistik, Universität Konstanz, 78457 Konstanz, Germany

Received 30 August 2004

Available online 18 March 2005

Communicated by Eva Bayer-Fluckiger

Abstract

Let $g_1, \dots, g_r \in \mathbb{R}[x_1, \dots, x_n]$ such that the set $K = \{g_1 \geq 0, \dots, g_r \geq 0\}$ in \mathbb{R}^n is compact. We study the problem of representing polynomials f with $f|_K \geq 0$ in the form $f = s_0 + s_1 g_1 + \dots + s_r g_r$ with sums of squares s_i , with particular emphasis on the case where f has zeros in K . Assuming that the quadratic module of all such sums is archimedean, we establish a local–global condition for f to have such a representation, vis-à-vis the zero set of f in K . This criterion is most useful when f has only finitely many zeros in K . We present a number of concrete situations where this result can be applied. As another application we solve an open problem from [S. Kuhlmann et al., Positivity, sums of squares and the multi-dimensional moment problem II, Adv. Geometry, in press] on one-dimensional quadratic modules.

© 2005 Elsevier Inc. All rights reserved.

Keywords: Non-negative polynomials; Sums of squares; Positivity; Quadratic modules; Semiorderings; Real algebraic geometry

Introduction

Assume that we are given polynomials g_1, \dots, g_r with real coefficients in n variables, and another such polynomial f which is non-negative on the subset $K := \{g_1 \geq 0, \dots,$

E-mail address: claus.scheiderer@uni-konstanz.de.

$g_r \geq 0\}$ of \mathbb{R}^n . We are studying the problem of representing f in the form

$$f = s_0 + s_1 g_1 + \cdots + s_r g_r, \quad (*)$$

where the s_i are sums of squares of polynomials. Such representations of f have been considered by several authors, starting with Putinar [11]. They were called *distinguished representations* by Jacobi and Prestel [5,10], a terminology which we adopt here.

Let us record what is known about this question. Write M for the subset of $\mathbb{R}[x_1, \dots, x_n]$ which consists of all sums $(*)$ (M is called the quadratic module generated by g_1, \dots, g_r). First let us assume that M is a preordering, i.e. is multiplicatively closed. Then, if K is compact, every f which is strictly positive on K has a representation $(*)$ (Schmüdgen's theorem [17]). If f is only assumed to be non-negative on K , there is a local–global criterion for the existence of an identity $(*)$ [14]. It refers to the zero set of f in K and is most useful when this set is discrete, hence finite. In this case, the existence of an identity $(*)$ follows from the existence of such identities in the completed local rings of the zeros of f in K .

We only mention that, in the context of preorderings, much is known for non-compact K as well, both positive and negative results (see [12,14,15] and forthcoming work).

Now let us drop the assumption that M is multiplicatively closed. Then compactness of K alone does not in general suffice any more to guarantee that M contains all polynomials strictly positive on K . What is needed is that M is archimedean. This condition is stronger than compactness of K , and is of arithmetic rather than geometric nature. That it is (not only necessary but also) sufficient was proved by Jacobi [4]. The problem of verifying the archimedean hypothesis is often subtle in concrete situations. It is directly related to quadratic form theory and to the Bröcker–Prestel local–global criterion for weak isotropy. From this theorem, Jacobi and Prestel have obtained valuation-theoretic criteria for M to be archimedean ([5], see also [10]). Despite their abstract appearance, they are often very useful and applicable.

The aim of this note is to study possible extensions of Jacobi's theorem to polynomials which have zeros in K (and are non-negative on K). This is done in a spirit similar to the work on preorderings [14] which we recalled before. Now the main technical result is Theorem 2.8. Roughly, if we assume that M is archimedean and the zero set of f in K is finite, it says again that the existence of identities $(*)$ in the completed local rings of the zeros implies $f \in M$. However, what is really needed is a certain condition (condition (2) in Theorem 2.8), which is stronger than discreteness of the zeros of f in K . Again, it is a condition of arithmetic nature.

In order to apply the criterion, we need to discuss this condition (2). We do this at the beginning of Section 2, and establish a number of purely geometric hypotheses which are sufficient for (2).

The paper is organized as follows. After a notation and preliminaries section, the proof of the local–global criterion in Theorem 2.8 occupies Section 1. Similarly as in [14], we choose to present this result in an “abstract” setting, namely for arbitrary (noetherian) rings, using the language of the real spectrum. This is done to allow applications to other interesting situations as well, like representations $(*)$ over number fields. The entire Section 2 deals with the “geometric” situation, polynomials over the field of real numbers. Here we discuss various concrete situations to which the criterion applies.

Section 3 is concerned with another application of the local–global criterion, prompted by a question of Kuhlmann, Marshall and Schwartz [8]: does there exist a quadratic module M in $\mathbb{R}[x] = \mathbb{R}[x_1]$ which is not a preordering, but whose associated set K is compact? (When K is allowed to be non-compact, or when $n \geq 2$, the answer is well known to be yes.) We discuss this question more generally on algebraic curves, and use our main result to show that the answer is no if the curve has no real singular points (Corollary 4.4). On the other hand, the answer is yes if the curve has a non-isolated real singular point (Corollary 4.6).

One word about the methods. It is a characteristic feature of quadratic modules that their study requires structures which are more general than orderings, namely semiorderings. In contrast, semiorderings usually play no role in the study of quadratic modules which are multiplicatively closed (preorderings). The interplay between semiorderings and the geometry is not as close as it is for orderings, where the Artin–Lang principle makes the relation very tight. The failure of this principle for semiorderings is the reason why we encounter conditions of “arithmetic” nature that cannot be translated into geometric properties.

I am indebted to Murray Marshall for valuable comments on a preliminary version.

1. Notation and preliminaries

All rings are commutative and have a unit. If A is a local ring and \mathfrak{m} is its maximal ideal, \hat{A} denotes the completion of A with respect to the \mathfrak{m} -adic topology.

1.1. We use the language of the real spectrum, for which we refer to the well-known text books, in particular to [2,6,10]. The last one is particularly recommended for more background on semiorderings. A recent survey on positivity and sums of squares issues is [15].

By a *quadratic module* in A we mean a subset M of A which satisfies $1 \in M$, $M + M \subset M$ and $a^2M \subset M$ for every $a \in A$. (Note that we allow the degenerate case $-1 \in M$.) The *support* of M is $\text{supp}(M) = M \cap (-M)$. If $\frac{1}{2} \in A$, this is an ideal of A .

The quadratic module M is called a *preordering* of A if it is multiplicatively closed, i.e. if $MM \subset M$. If T is a preordering, a *T -module* is a quadratic module M with $TM \subset M$. Thus a quadratic module is the same thing as a T_0 -module, where $T_0 := \Sigma A^2$ is the preordering of all sums of squares in A .

The smallest quadratic module containing a given subset X of A is denoted $QM(X)$, and is called the quadratic module generated by X .

A quadratic module S in A is called a *semiordering* of A if $S \cup (-S) = A$, and if $\text{supp}(S)$ is a prime ideal of A . An *ordering* of A is a semiordering which is also a preordering. With respect to a semiordering S , every element of A has a unique sign in $\{-1, 0, 1\}$. Notations like $f >_S 0$ or $f \geq_S 0$ are therefore self-explaining. The sign is compatible with addition, but not with multiplication unless S is an ordering.

The *semireal spectrum* of A is the topological space $\text{SSper}(A)$ consisting of all semiorderings of A , where the topology is generated by the subsets $\{S: f >_S 0\}$ ($f \in A$). The *real spectrum* of A is the subspace $\text{Sper}(A)$ of $\text{SSper}(A)$ consisting of all orderings.

Often we will denote (semi-) orderings by letters like α , and write $f(\alpha) > 0$, $f(\alpha) \geq 0$ instead of $f >_\alpha 0$, $f \geq_\alpha 0$, to emphasize the character of the ring elements as generalized functions on the (semi-) real spectrum.

1.2. Let M be a quadratic module in A . Associated with M are the closed subset

$$\mathcal{Y}_M := \{\beta \in \text{SSper}(A) : f(\beta) \geq 0 \text{ for every } f \in M\}$$

of $\text{SSper}(A)$ and the closed subset

$$\mathcal{X}_M := \{\alpha \in \text{Sper}(A) : f(\alpha) \geq 0 \text{ for every } f \in M\}$$

of $\text{Sper}(A)$.

1.3. The following notion is of central importance. A quadratic module M in A is *archimedean* if $A = \mathbb{Z} + M$. In terms of the partial ordering on A defined by $f \leq_M g : \Leftrightarrow g - f \in M$, this means that every ring element is bounded in absolute value by an integer.

2. The main result

Let always A be a ring. Given $f \in A$, we write $Z(f) := \{\alpha \in \text{Sper } A : f(\alpha) = 0\}$.

The key step for the local–global principle in [14] was Proposition 2.5. We first need to generalize this result from preorderings to quadratic modules.

Proposition 2.1. *Assume $\frac{1}{n} \in A$ for some $n > 1$. Let T be a preordering in A , and let M be an archimedean T -module. Let $f \in A$ with $f \geq 0$ on \mathcal{X}_M , and assume there is an identity*

$$f = s + bt$$

with $s \in M$, $t \in T$ and $b \in A$. Suppose further that $b > 0$ on $Z(f) \cap \mathcal{X}_M$. Then $f \in M$.

Proof. The proof is a variant of the proof of [14, 2.5]. Consider $X = \mathcal{X}_M^{\max}$, the space of closed points of \mathcal{X}_M . This is a compact (Hausdorff) topological space. Recall that since M is archimedean, every element f of A induces a continuous function $\Phi(f) : X \rightarrow \mathbb{R}$ by evaluation. By the Stone–Weierstraß theorem, the image of the ring homomorphism $\Phi : A \rightarrow C(X, \mathbb{R})$ is dense with respect to uniform approximation. (See [10, 5.2] or [14, 2.2.1] for more details.). To keep notation simple, we will write $f(x)$ instead of $\Phi(f)(x)$, for $f \in A$ and $x \in X$.

We are going to apply [14, Lemma 2.6] with $n = 1$, $a = \Phi(st)$ and $u = \Phi(2s)$, and have to check the hypotheses of this lemma. Clearly $a \geq 0$ on X . For the second condition we need to show that for every $x \in X$ there exists a real number y satisfying

$$s(x)y \cdot (2 + t(x)y) < b(x).$$

This is indeed true, by a similar argument as in [14]: if $s(x) = 0$, one easily sees $b(x) > 0$. If $s(x) > 0$ we may assume $t(x) > 0$. We have $f(x) > 0$, and the desired inequality gets transformed into

$$(1 + t(x)y)^2 < \frac{f(x)}{s(x)}$$

by multiplication with $t(x)$. This is clearly satisfied for suitable y .

From [14, Lemma 2.6] we conclude that there exists a continuous function $\eta: X \rightarrow \mathbb{R}$ satisfying

$$s(x)\eta(x) \cdot (2 + t(x)\eta(x)) < b(x)$$

for all $x \in X$. Approximating η sufficiently closely, we see that there exists $v \in A$ with

$$sv(2 + tv) < b$$

on X , and hence on \mathcal{X}_M . So Jacobi's Positivstellensatz ([4], [10, 5.3.7]), together with $\frac{1}{n} \in A$, implies $b - sv(2 + tv) \in M$, from which we get $f \in M$ since

$$f = s + bt = (1 + tv)^2 s + t(b - sv(2 + tv)). \quad \square$$

Remark 2.2. 1. Marshall has found an elegant different approach to Propositions 2.1 and 2.3, based on [8, Lemma 2.1]. See his recent preprint [9].

2. With a finer argumentation one gets additional information as in [14, Remark 2.7]. Since we are not going to use this here, we will not go into it.

3. Schweighofer [16] has found a substantial generalization of [14, Proposition 2.5] (which is the special case $M = T$ of Proposition 2.1). In his version, M can be any archimedean semiring in A , and the condition $f = s + bt$ from 2.1 is weakened to a condition of the form $f = \sum_i b_i t_i$.

As a direct application of Proposition 2.1 we get the following analogue of [14, Corollary 3.11].

Proposition 2.3. *Let A be a ring containing $\frac{1}{2}$, let M be an archimedean quadratic module in A , and let $f \in A$ with $f \geq 0$ on \mathcal{X}_M . If $f \in M + f\sqrt{(f)}$, then $f \in M$.*

Proof. We have $f = x + fh$, i.e. $f(1 - h) = x$, with $x \in M$ and $h \in \sqrt{(f)}$. Modulo the ideal (f^3) of A , $1 - h$ is a unit square. Hence there is $a \in A$ with

$$f \equiv a^2 x \pmod{(f^3)}.$$

Similarly, there is $b \in A$ with

$$1 - f \equiv b^2 \pmod{(f^3)}.$$

Multiplying these two we get $f - f^2 = (ab)^2x + cf^3$ with some $c \in A$, i.e.

$$f = (ab)^2x + f^2(1 + cf).$$

Now $f \in M$ follows from Proposition 2.1. \square

Here is the analogue of [14, Theorem 3.13].

Proposition 2.4. *Let A be a ring containing $\frac{1}{2}$, let M be an archimedean quadratic module in A , and let $f \in A$ with $f \geq 0$ on \mathcal{X}_M . If $f \in M + J$ for every ideal J of A with $\sqrt{J} = \sqrt{\text{supp}(M + (f))}$, then $f \in M$.*

Remark 2.5. *For every ideal I of A we have*

$$\sqrt{\text{supp}(M + I)} = \sqrt{\text{supp}(M + {}^{\text{re}}\sqrt{I})},$$

and this is a real radical ideal. Indeed, by the Nullstellensatz for quadratic modules (see [15, 1.4.6.1]) one has

$$\sqrt{\text{supp}(M + I)} = \bigcap_{\beta \in \mathcal{Y}_{M+I}} \text{supp}(\beta)$$

which is a real radical ideal. Moreover, for any semiordering β of A ,

$$\begin{aligned} \beta \in \mathcal{Y}_{M+I} &\Leftrightarrow \beta \in \mathcal{Y}_M \text{ and } I \subset \text{supp}(\beta) \\ &\Leftrightarrow \beta \in \mathcal{Y}_M \text{ and } {}^{\text{re}}\sqrt{I} \subset \text{supp}(\beta) \Leftrightarrow \beta \in \mathcal{Y}_{M+{}^{\text{re}}\sqrt{I}}, \end{aligned}$$

from which we get the asserted equality.

Proof of Proposition 2.4. By Remark 2.5, the radicals of $\text{supp}(M + (f))$ and of $\text{supp}(M + (f^2))$ coincide. Choose a family $(g_\lambda)_{\lambda \in \Lambda}$ of elements of $\text{supp}(M + (f^2))$ with

$$\sqrt{\text{supp}(M + (f))} = \sqrt{(f) + (g_\lambda: \lambda \in \Lambda)}.$$

Let J be the ideal generated by f^2 and all the $(f + g_\lambda)^2$. Then $\sqrt{J} = \sqrt{\text{supp}(M + (f))}$, and so $f \in M + J$ by the hypothesis. Hence we have

$$f \in M + (f^2, (f + g_1)^2, \dots, (f + g_r)^2)$$

for finitely many g_1, \dots, g_r among the g_λ . Assume $r \geq 1$, let

$$\tilde{M} := M + (f^2, (f + g_1)^2, \dots, (f + g_{r-1})^2)$$

and let $\tilde{f} := f + g_r$. Then \tilde{M} is an archimedean quadratic module, and \tilde{f} is non-negative

(in fact, identically zero) on $\mathcal{X}_{\tilde{M}}$. We have $f \in \tilde{M} + (\tilde{f}^2)$ and $g_r \in M + (f^2) \subset \tilde{M}$, hence $\tilde{f} \in \tilde{M} + (\tilde{f}^2)$. So Proposition 2.3 implies $\tilde{f} \in \tilde{M}$. Since $-g_r \in M + (f^2) \subset \tilde{M}$, also $f \in \tilde{M}$. Now we can iterate this argument, arriving at $f \in M + (f^2)$. A final application of Proposition 2.3 gives $f \in M$. \square

Remark 2.6. Proposition 2.4 continues to hold if the condition $f \in M + J$ is instead required for every ideal J with $\sqrt{J} = \sqrt[r]{(f)}$. Indeed, this is an a priori stronger hypothesis than the original one, since for an ideal I with $\sqrt{I} = \sqrt{\text{supp}(M + (f))}$ we can put $J := I \cap \sqrt[r]{(f)}$ and have $\sqrt{J} = \sqrt[r]{(f)}$ by Remark 2.5.

As in the case for preorderings [14], Proposition 2.4 is most useful when the ideal $\text{supp}(M + (f))$ is zero-dimensional. (By the *dimension* of an ideal I in a ring A we mean the Krull dimension of the ring A/I .) Before we study this case in greater detail, we observe the following.

Lemma 2.7. *Let N be any quadratic module in A . The following conditions are equivalent:*

- (i) $\text{supp}(N)$ has dimension ≤ 0 ;
- (ii) $\text{supp}(\beta)$ is a maximal ideal for every semiordering β in \mathcal{Y}_N .

Moreover, if they are satisfied, and if the ring A is noetherian, the set of maximal ideals $\{\text{supp}(\beta) : \beta \in \mathcal{Y}_N\}$ is finite.

Proof. We have $\text{supp}(N) = \bigcap_{\beta \in \mathcal{Y}_N} \text{supp}(\beta)$, from which (i) \Rightarrow (ii) is clear. For the converse recall that \mathcal{Y}_N is a spectral space and the support map $\mathcal{Y}_N \rightarrow \text{Spec } A$ is spectral. Hence the subset $\{\text{supp}(\beta) : \beta \in \mathcal{Y}_N\}$ of $\text{Spec } A$ is pro-constructible. Assuming that it consists of maximal ideals, it is therefore a closed set, being stable under specialization. Hence it is equal to the closed set $\mathcal{V}(\text{supp } N)$ in $\text{Spec } A$. This implies (i), and it also implies the last statement in the noetherian case. \square

Given a quadratic module M in A and a prime ideal \mathfrak{p} in A , we write $\widehat{M}_{\mathfrak{p}}$ for the quadratic module which is generated by (the image of) M in the completed local ring $\widehat{A}_{\mathfrak{p}}$.

Theorem 2.8. *Let A be a noetherian ring with $\frac{1}{2} \in A$, and let M be a quadratic module in A . Let $f \in A$ with $f \geq 0$ on \mathcal{X}_M . Assume that the following two conditions hold:*

- (1) M is archimedean;
- (2) the ideal $\text{supp}(M + (f))$ has dimension ≤ 0 .

Then, if $f \in \widehat{M}_{\text{supp}(\alpha)}$ for every $\alpha \in \mathcal{X}_{M+(f)}$, this implies $f \in M$.

Proof. Let $\beta \in \mathcal{Y}_{M+(f)}$. By hypothesis, $\text{supp}(\beta)$ is a maximal ideal (see Lemma 2.7). Therefore we have β is a maximal semiordering of A . Being archimedean, it is an ordering

(see [10, 5.3.5]), hence β lies in $\mathcal{X}_{M+(f)}$. The Nullstellensatz for quadratic modules therefore gives us

$$\sqrt{\operatorname{supp}(M+(f))} = \bigcap_{\beta \in \mathcal{Y}_{M+(f)}} \operatorname{supp}(\beta) = \bigcap_{\alpha \in \mathcal{X}_{M+(f)}} \operatorname{supp}(\alpha) = \mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_r,$$

where we denote by $\mathfrak{m}_1, \dots, \mathfrak{m}_r$ the maximal ideals $\operatorname{supp}(\alpha)$, $\alpha \in \mathcal{X}_{M+(f)}$.

For every $i = 1, \dots, r$ we have $f \in \widehat{M}_{\mathfrak{m}_i}$ by assumption, which implies $f \in M + \mathfrak{m}_i^N$ for every $N \geq 1$. By the Chinese Remainder Theorem,

$$\bigcap_i (M + \mathfrak{m}_i^N) = M + \bigcap_i \mathfrak{m}_i^N,$$

and so $f \in M + \bigcap_i \mathfrak{m}_i^N$ for every $N \geq 0$. Hence $f \in M + J$ for every ideal J of A with $\sqrt{J} = \sqrt{\operatorname{supp}(M+(f))}$, and we conclude $f \in M$ from Proposition 2.4. \square

Remark 2.9. 1. Some caution is in order, since the situation is more subtle than in the case of preorderings: the support ideal $\operatorname{supp}(M+(f))$ can be smaller than is suggested by the “geometry” (namely the real spectrum). See Section 3.1.

2. Condition (2) in Theorem 2.8 says that $\operatorname{supp}(\beta)$ is a maximal ideal for every $\beta \in \mathcal{Y}_{M+(f)}$ (Lemma 2.7). Since conditions (1) and (2) imply that every $\beta \in \mathcal{Y}_{M+(f)}$ is in fact an ordering, one may wonder whether (2) can be replaced by the weaker condition that $\operatorname{supp}(\alpha)$ is a maximal ideal for every $\alpha \in \mathcal{X}_{M+(f)}$. This latter condition would be much easier to check, since it only depends on the geometry of the situation.

However, this seems quite unlikely. The weaker condition definitely does not imply the stronger condition (2), not even when M is archimedean; see Section 3.1 and Example 3.2 for a broader discussion. On the other hand, the proof of Theorem 2.8 uses condition (2) in an essential way.

3. Applications in the geometric case

By “geometric case” we mean that A is a finitely generated \mathbb{R} -algebra and $M = QM(g_1, \dots, g_r)$ is a finitely generated quadratic module in A . Associated with this data we have the affine \mathbb{R} -scheme $V := \operatorname{Spec}(A)$ and the basic closed semi-algebraic set

$$K := \mathcal{S}(M) := \{x \in V(\mathbb{R}) : g_1(x) \geq 0, \dots, g_r(x) \geq 0\}$$

in $V(\mathbb{R})$, the space of real points of V . Let $f \in A$ with $f \geq 0$ on K . Theorem 2.8 provides sufficient conditions for $f \in M$. We are going to discuss concrete situations to which they apply.

Given $f \in A$, we always write $\mathcal{Z}(f)$ for the set of zeros of f in $V(\mathbb{R})$. Everything in this section and the next remains true if \mathbb{R} is replaced by a real closed subfield of \mathbb{R} .

3.1. We first have to discuss how conditions (1) and (2) in Theorem 2.8 can be checked. This is more subtle than in the case of preorderings. To highlight the difference, let us for a moment assume that $M = T$ is a preordering, i.e. is multiplicatively closed. Then T archimedean is equivalent to K compact, by Wörmann's formulation of Schmüdgen's theorem [1]. Moreover, the dimension of the ideal $\text{supp}(T + (f))$ is simply the dimension of the semi-algebraic set $\mathcal{Z}(f) \cap K$ (e.g. [14, Remark 3.12]). So conditions (1) and (2) say that K is compact and f has only finitely many zeros in K .

Now we drop the assumption that M is multiplicatively closed, so M is just a quadratic module. Then (1) and (2) are no longer reflected by the geometry of the situation alone. Compactness of K is necessary for M archimedean, but not in general sufficient. Recall that, if $A = \mathbb{R}[V]$ is generated as \mathbb{R} -algebra by x_1, \dots, x_n , then M is archimedean if and only if there exists a real number c with $c - \sum_i x_i^2 \in M$. Even if this is the case, it may be hard to realize if M is just given in terms of a system of generators g_1, \dots, g_r , as above. One possible way of verifying the archimedean condition is through the valuative criterion of Jacobi–Prestel [10, Theorem 6.2.2(2)].

Jacobi and Prestel provide some *purely geometric* conditions which are sufficient for M to be archimedean. One nice example is this: if A is the polynomial ring over \mathbb{R} , and if M is generated by polynomials g_1, \dots, g_r whose degrees have all the same parity modulo 2, then M is archimedean provided that the cone $\{\tilde{g}_1 \geq 0, \dots, \tilde{g}_r \geq 0\}$ defined by the leading forms (= highest degree forms) \tilde{g}_i of the generators is reduced to $\{0\}$ (see [5] or [10, 6.3.4(i)]).

See also Proposition 4.1 for a geometric condition which implies that M is archimedean.

Assuming now that M is archimedean, Jacobi's Positivstellensatz ([4], [10, 5.3.7]) implies that M contains every $f \in A$ with $f > 0$ on K . In a first approximation, Theorem 2.8 says that $f \in M$ remains true if f is only assumed to be non-negative on K , with $\mathcal{Z}(f) \cap K$ being finite, and if there is no local obstruction in (the completed local ring of) any of the zeros of f in K .

But condition (2) in Theorem 2.8 is stronger than finiteness of $\mathcal{Z}(f) \cap K$: the dimension of the ideal $\text{supp}(M + (f))$ can be greater than the dimension of $\mathcal{Z}(f) \cap K$, even if M is archimedean. See Example 3.2 for an example. So the “first approximation” we have just stated is not quite correct.

Example 3.2. Let M be the quadratic module in $A = \mathbb{R}[x, y]$ generated by the four polynomials

$$1 - x^2 - y^2, \quad -xy, \quad x - y, \quad y - x^2.$$

Then M is archimedean since $1 - x^2 - y^2 \in M$, and the set $K = \mathcal{S}(M)$ consists only of the origin. So the geometry shows a 0-dimensional picture. But we have $\text{supp}(M) = (0)$. More precisely, the quotient field $F = \mathbb{R}(x, y)$ of A has a semiordering which contains M .

Indeed, consider the quadratic form

$$q = \langle 1, 1 - x^2 - y^2, -xy, x - y, y - x^2 \rangle$$

over F . Let v be a valuation of F with residue field \mathbb{R} whose value group is a subgroup of the ordered group $(\mathbb{R}, +)$, such that

$$0 < v(x) < v(y) < 2v(x)$$

and $v(x), v(y)$ are \mathbb{Z} -linearly independent. Then all residue forms of q with respect to v are strongly anisotropic. So q is strongly anisotropic over the henselization of (F, v) and, a fortiori, over F itself. This means that F has a semiordering S with $M \subset S$ [10, Lemma 6.1.1].

3.3. For practical purposes, it may be hard to decide whether condition (2) of Theorem 2.8 is satisfied. One may reformulate the condition as follows:

Assume $M = QM(g_1, \dots, g_r)$ with $g_i \in A$. Then $\text{supp}(M + (f))$ has dimension ≤ 0 if and only if for every non-maximal real prime ideal \mathfrak{p} of A containing f , the quadratic form $\langle 1, g_1, \dots, g_r \rangle_{\mathfrak{p}}^$ over the residue field $\kappa(\mathfrak{p})$ is weakly isotropic.*

(Here $\langle \dots \rangle_{\mathfrak{p}}^*$ denotes the quadratic form obtained by reducing the entries modulo \mathfrak{p} and leaving away all zeros.) Using the Bröcker–Prestel local–global principle, one may give still another equivalent formulation, using valuations on the residue fields $\kappa(\mathfrak{p})$.

In the next result we isolate two conditions of geometric nature which imply condition (2) of Theorem 2.8. Again, A is a finitely generated \mathbb{R} -algebra, $V = \text{Spec } A$, M is a finitely generated quadratic module in A and $K = \mathcal{S}(M) \subset V(\mathbb{R})$.

Proposition 3.4. *Assume that $f \in A$ is non-negative on K and has only finitely many zeros in K . If M is archimedean, and if $f \in \widehat{M}_p$ for every $p \in \mathcal{Z}(f) \cap K$, then $f \in M$, provided that at least one of the following two conditions is satisfied:*

- (1) $\dim \mathcal{Z}(f) \leq 1$;
- (2) *for every $p \in \mathcal{Z}(f) \cap K$ there are a neighborhood U of p in $V(\mathbb{R})$ and an element $a \in M$ such that $\{a \geq 0\} \cap \mathcal{Z}(f) \cap U \subset K$.*

Proof. According to Theorem 2.8 and Lemma 2.7, we have to show, for every $\beta \in \mathcal{Y}_{M+(f)}$, that $\mathfrak{q} := \text{supp}(\beta)$ is a maximal ideal of A .

Condition (1) implies $\dim(A/\mathfrak{q}) \leq 1$. Therefore the residue field $\kappa(\mathfrak{q})$ is an SAP field, which means that every semiordering of $\kappa(\mathfrak{q})$ is an ordering. This applies in particular to β . Hence β lies in $\mathcal{Z}(f) \cap K = \mathcal{Z}(f) \cap K$, and \mathfrak{q} is a maximal ideal.

Now assume the second condition. Since M is archimedean, β specializes to an ordering [10, 5.3.5], hence to a point $p \in \mathcal{Z}(f) \cap K$. Let $a \in M$ with

$$(\{a \geq 0\} \cap \mathcal{Z}(f))_p \subset K_p \quad (*)$$

as set germs around p . We have $a \geq_{\beta} 0$ since $a \in M$. Now Lemma 3.5 below shows that there exists an ordering $\alpha \in \text{Sper } A$ which specializes to p , such that $\text{supp}(\alpha) = \mathfrak{q}$ and

$a(\alpha) \geq 0$. By $(*)$ we have $\alpha \in \widetilde{K}$, and therefore $\alpha \in \widetilde{\mathcal{Z}(f)} \cap K$. Since $\mathcal{Z}(f) \cap K$ is finite, it follows that $\alpha = p = \beta$, and we are done. \square

Lemma 3.5. *Let A be a ring, let $\gamma \in \text{Sper } A$, and let β be a semiordering of A which specializes to γ . Moreover, let $a \in A$ with $a \geq_\beta 0$. Then there exists an ordering $\alpha \in \text{Sper } A$ which specializes to γ , and which satisfies $\text{supp}(\alpha) = \text{supp}(\beta)$ and $a \geq_\alpha 0$.*

Proof. We can assume $\text{supp}(\beta) = (0)$, by replacing A with $A/\text{supp}(\beta)$. Let $Q = \{f \in A : f(\gamma) > 0\}$. Then $f >_\beta 0$ for every $f \in Q$, since β specializes to γ . Let K be the quotient field of A . We can regard β as a semiordering of K , and write $S = \{f \in K : f \geq_\beta 0\}$ for the associated cone. Let T be the quadratic module generated by Q in K . Then $T \subset S$ since $Q \subset S$. Moreover, T is a preordering since Q is multiplicatively closed. Therefore, T is the intersection of all orderings of K which contain Q . In particular, there is an ordering $\alpha \in \text{Sper } A$ specializing to γ with $\text{supp}(\alpha) = (0)$. Moreover, if $a \neq 0$, then $-a \notin S$, which implies that there is such α with $a \geq_\alpha 0$. \square

Here are a few sample applications of Proposition 3.4.

Corollary 3.6. *Let V be a non-singular affine \mathbb{R} -variety, and let M be a finitely generated quadratic module in $\mathbb{R}[V]$ which is archimedean. Let $f \in \mathbb{R}[V]$ satisfy $f \geq 0$ on $K := \mathcal{S}(M)$, and assume that, for every $p \in \mathcal{Z}(f) \cap K$, f is non-negative on a neighborhood of p and the Hessian $D^2 f(p)$ is positive definite. Then $f \in M$.*

(We understand the Hessian $D^2 f(p)$ in a naive sense, for example as calculated with respect to a local parameter system at p .)

Proof. The positive definiteness of the Hessians implies, for every $p \in \mathcal{Z}(f) \cap K$, that f is a sum of squares in the completed local ring $\widehat{\mathcal{O}}_{V,p}$ at p (see [14, 3.18]). Moreover, it ensures that every $p \in \mathcal{Z}(f) \cap K$ is an isolated zero of f . Hence condition (2) of Proposition 3.4 is fulfilled, and we can conclude by this proposition. \square

Corollary 3.7. *Let V be a non-singular affine surface over \mathbb{R} , and let $M = QM(g_1, \dots, g_r)$ be an archimedean quadratic module in $\mathbb{R}[V]$, where the g_i are such that the curves $C_i = \{g_i = 0\}$ are reduced and no two of them share an irreducible component.*

Let $f \in \mathbb{R}[V]$ be non-negative on $K = \mathcal{S}(M)$. Assume that the set $\mathcal{Z}(f) \cap K$ is finite and does not contain a singular point of the curve $C_1 \cup \dots \cup C_r$. Then $f \in M$.

Proof. We can apply Proposition 3.4 as soon as we know $f \in \widehat{M}_p$ for $p \in \mathcal{Z}(f) \cap K$. So let $p \in \mathcal{Z}(f) \cap K$. The local ring $A := \mathcal{O}_{V,p}$ is regular of dimension 2, hence every psd element in $\widehat{A} \cong \mathbb{R}[[x, y]]$ is a sum of (two) squares ([3], see also [13]). If p lies in the interior of K then f is psd in \widehat{A} , hence is a sum of squares in \widehat{A} . Otherwise there exists an index i with $g_i(p) = 0$. Since p is a regular point on $\bigcup_j C_j$ we have $g_i \notin \mathfrak{m}_A^2$ and $g_j(p) > 0$ for every $j \neq i$. So the ring $A' := A[\sqrt{g_i}]$ is again local and regular of dimension 2, and f is psd in \widehat{A}' , hence a sum of squares in \widehat{A}' . This implies that f lies in the preordering generated by g_i in \widehat{A} , and in particular, $f \in \widehat{M}_p$. \square

Here is a particularly concrete example.

Corollary 3.8. *Let g_1, \dots, g_r be linear polynomials in $\mathbb{R}[x, y]$ such that the convex polygon $K = \{g_1 \geq 0, \dots, g_r \geq 0\}$ is compact with non-empty interior. Let f be a polynomial which is non-negative on K . If f does not vanish in any vertex of K , then f has a representation*

$$f = s_0 + s_1 g_1 + \dots + s_r g_r$$

where the s_i are sums of squares of polynomials.

Proof. Consider the quadratic module $M := QM(g_1, \dots, g_r)$. Then M is archimedean by a famous result of Minkowski: choose $c \in \mathbb{R}$ such that $|x| \leq c$ and $|y| \leq c$ on K ; Minkowski's theorem implies that $c \pm x$ and $c \pm y$ are non-negative linear combinations of 1 and the g_i , and hence lie in M . Write $f = f_1 f_2^2$ where f_1, f_2 are polynomials and f_1 is square-free. Then $f_1 \geq 0$ on K , and $\mathcal{Z}(f_1) \cap K$ is finite. Hence Corollary 3.7 can be applied to f_1 , showing $f_1 \in M$. \square

Remark 3.9. The condition that f does not vanish in any vertex of K cannot be avoided. For example, the quadratic module $M = QM(x, y, 1 - x - y)$ is archimedean. It is easy to see that M does not contain any polynomial of the form $f = xy + \sum_{i+j \geq 3} a_{ij} x^i y^j$. But one can find such f with $f|_K \geq 0$ for which $\mathcal{Z}(f) \cap K$ consists only of the origin, for example $f = xy + x^3 + y^3$.

Corollary 3.10. *Let V be a non-singular affine surface over \mathbb{R} , and let M be an archimedean quadratic module in $\mathbb{R}[V]$. Let $f \in \mathbb{R}[V]$ be non-negative on $K = \mathcal{S}(M)$. If each $p \in \mathcal{Z}(f) \cap K$ is an isolated zero of f in $V(\mathbb{R})$, but not an isolated point of K , then $f \in M$.*

Proof. Clearly, $\mathcal{Z}(f) \cap K$ is finite, and condition (2) of Proposition 3.4 is satisfied. So it suffices to show $f \in \widehat{M}_p$ for every $p \in \mathcal{Z}(f) \cap K$. The regular function f does not change sign locally around p , since p is an isolated zero of f . The condition that p is not an isolated point of K ensures $f \geq 0$ around p . Therefore f is a sum of squares in $\widehat{\mathcal{O}}_p$. \square

4. Quadratic modules which are preorderings

Let M be a quadratic module in an affine \mathbb{R} -variety V with $\dim \text{supp}(M) \leq 1$, and assume that the set $K = \mathcal{S}(M)$ is compact. We are asking: does this implies that M is a preordering? We shall apply the local–global principle for quadratic modules to give the answer.

A necessary condition for M to be a preordering is that M is archimedean (Schmüdgen's theorem). This condition holds indeed:

Proposition 4.1 [5]. *Let A be a finitely generated \mathbb{R} -algebra, $V = \operatorname{Spec} A$, and let M be a finitely generated quadratic module in A with $\dim \operatorname{supp}(M) \leq 1$. If the set $K = \mathcal{S}(M)$ is compact, then M is archimedean.*

Proof. (See also [5, Remark 4.7] for a different proof.) We can replace A by $A/\operatorname{supp}(M)$, therefore we can assume that A has dimension ≤ 1 (and is possibly non-reduced). Let M be generated by g_1, \dots, g_r . We will apply the valuation-theoretic criterion in [10, 6.2.2].

Let \mathfrak{p} be a prime ideal of A with $\dim(A/\mathfrak{p}) = 1$, and write C for the curve $C = \operatorname{Spec}(A/\mathfrak{p})$. Let v be a real valuation of its function field $\mathbb{R}(C)$ without centre in C . Then v is the valuation associated to some real point of C at infinity, and is discrete of rank one. Let α_1, α_2 be the two orderings of $\mathbb{R}(C)$ which are compatible with v . Since K is compact, neither of them lies in \tilde{K} . Therefore, either there is an index i with $g_i(\alpha_v) < 0$ for $v = 1, 2$; then $v(g_i)$ is even, and the first residue form of the quadratic form $q := \langle 1, g_1, \dots, g_r \rangle$ contains $\langle 1, -1 \rangle$. Or, there are indices $i \neq j$ such that g_i and g_j change sign in $\{\alpha_1, \alpha_2\}$ and $(g_i g_j)(\alpha_v) < 0$ for $v = 1, 2$. In that case, the second residue form of q contains the form $\langle 1, -1 \rangle$. In any case, q has an isotropic residue form. From the above-mentioned criterion it follows therefore that M is archimedean. \square

Now we apply the local–global principle to the question raised at the beginning of this section.

Proposition 4.2. *Let A be a Dedekind domain containing $\frac{1}{2}$, and assume that for every maximal ideal \mathfrak{m} of A the residue field A/\mathfrak{m} has at most one ordering. Then every archimedean quadratic module in A is a preordering.*

Proof. Let M be an archimedean quadratic module in A , let $0 \neq f, g \in M$. We have to show $fg \in M$. Hypotheses (1) and (2) of Theorem 2.8 are satisfied. So it suffices to show $fg \in \tilde{M}_{\mathfrak{m}}$ for every (real) maximal ideal \mathfrak{m} . By the Cohen structure theorem, we can therefore assume $A = k[[x]]$, where k is a field with exactly one ordering.

Since multiplication with unit squares does not affect the situation, we can assume $f = ax^m$ and $g = bx^n$, where $m, n \geq 1$ and $a, b \in k^*$. First assume that m is even. If $a > 0$ (with respect to the unique ordering of k), then f is a sum of squares in $k[[x]]$, and so $fg \in M$ is clear. If $a < 0$, then $f \in \operatorname{supp}(M)$, hence also $fg \in \operatorname{supp}(M)$ since $\operatorname{supp}(M)$ is an ideal in $k[[x]]$. By symmetry, we also get $fg \in M$ if n is even. Let finally m, n be odd. If $ab > 0$ then fg is a sum of squares. If $ab < 0$ then the one of f and g which has the larger order lies in $\operatorname{supp}(M)$. (If $m = n$, then both $f, g \in \operatorname{supp}(M)$.) So again $fg \in \operatorname{supp}(M)$. \square

Remark 4.3. 1. Proposition 4.2 becomes false as soon as A/\mathfrak{m} has two different orderings for some maximal ideal \mathfrak{m} . Indeed, this implies that the quotient field of A is not an SAP-field. Therefore, A has a semiordering with support (0) which is not an ordering.

2. Proposition 4.2 also becomes usually false if the quadratic module M is not archimedean. As a matter of fact, the univariate polynomial ring $A = \mathbb{R}[x]$ contains (non-archimedean) quadratic modules which are not preorderings, for example, the quadratic module generated by $x + 1$ and $x^2 - x$. (It is easy to verify this example directly; for a more systematic approach see [7, Theorem 2.5].)

Combining Propositions 4.1 and 4.2, we can now solve Open Problem 6 from [8]. This problem asks whether $\mathbb{R}[x]$ contains a quadratic module M which is not a preordering, but whose associated set $\mathcal{S}(M)$ in \mathbb{R} is compact. The answer is no, and we state it in greater generality:

Corollary 4.4. *Let C be an integral affine curve over \mathbb{R} , let M be a finitely generated quadratic module in $\mathbb{R}[C]$. Assume that the set $K = \mathcal{S}(M)$ is compact and does not contain a singular point of C . Then M is an archimedean preordering.*

Proof. M is archimedean according to Proposition 4.1. Let $0 \neq f, g \in M$, we show $fg \in M$. By Proposition 3.4 it suffices to show $fg \in \widehat{M}_p$ for every point p in K . This is indeed true by Proposition 4.2, since p is a regular point on C . \square

Beyond the local–global principle, the proof was using the fact that every quadratic module in $\mathbb{R}[[x]]$ is a preordering. In order to explore whether Corollary 4.4 extends to curves with real singular points, let us examine this last property for the local rings of such singularities. The result is that it never holds, at least if we restrict to non-isolated real singular points.

Proposition 4.5. *Let A be a singular one-dimensional local noetherian ring. If $\text{Sper}(A)$ contains a non-closed point, then A contains a quadratic module which is not a preordering.*

The hypothesis that $\text{Sper}(A)$ contains a non-closed point says that there exists a specialization $\eta \rightarrow \xi$ in $\text{Sper}(A)$ for which $\mathfrak{p} := \text{supp}(\eta)$ is a minimal prime ideal and $\text{supp}(\xi) = \mathfrak{m}$. In particular, the residue field of A is real.

Proof. Let $k = A/\mathfrak{m}$, the residue field of A . We claim that \mathfrak{m} contains two elements f and g which are linearly independent modulo \mathfrak{m}^2 , such that $fg + \mathfrak{m}^3$ contains no sum of squares. Assuming this claim, the quadratic module M generated by f and g is not a preordering. Indeed, suppose $fg = a + bf + cg$ with $a, b, c \in \Sigma A^2$. Reduction modulo \mathfrak{m} shows $a \in \mathfrak{m} \cap \Sigma A^2 \subset \mathfrak{m}^2$. Reduction modulo \mathfrak{m}^2 shows $b, c \in \mathfrak{m}$ (and hence $b, c \in \mathfrak{m}^2$), using linear independence of f and g modulo \mathfrak{m}^2 . Therefore $fg \equiv a \pmod{\mathfrak{m}^3}$, contradicting the assumption.

To prove the claim, let $\eta \in \text{Sper}(A)$ be such that $\mathfrak{p} = \text{supp}(\eta)$ is a minimal prime ideal of A and η has a specialization with support \mathfrak{m} . Then η extends to the completion \widehat{A} of A [13, Lemma 3.3], which shows that \widehat{A} has a minimal prime ideal \mathfrak{p}_1 which is real. Therefore, the integral closure of $\widehat{A}/\mathfrak{p}_1$ is isomorphic to $k_1[[t]]$, where k_1 is a finite real extension of k . We conclude that there exists a ring homomorphism $\varphi: A \rightarrow k_1[[t]]$ with kernel \mathfrak{p} which makes the square

$$\begin{array}{ccc} A & \longrightarrow & k \\ \varphi \downarrow & & \downarrow \\ k_1[[t]] & \longrightarrow & k_1 \end{array}$$

commutative (the unlabeled arrows being the obvious ones).

Let $f \in \mathfrak{m}$ be such that $n := \text{ord } \varphi(f)$ is minimal (≥ 1), so $\varphi(f) = ut^n$ with a unit u . Choose any $g_1 \in \mathfrak{m}$ which is linearly independent from f modulo \mathfrak{m}^2 . (Such g_1 exists since A was assumed to be singular.) We have $\varphi(g_1) = bt^n$ with $b \in k_1[[t]]$. Choose $c \in k^*$ such that $|cb| < |\bar{u}|$ with respect to some ordering of k_1 , and put $g := -f + cg_1$. For any $h \in \mathfrak{m}^3$ we have

$$\varphi(fg + h) \equiv ut^n \cdot (-ut^n + cbt^n) = u(cb - u) \cdot t^{2n} \pmod{t^{3n}},$$

and the residue class of $u(cb - u)$ in k_1 is not a sum of squares. Therefore, $\varphi(fg + h)$ is not a sum of squares in $k_1[[t]]$. Hence $fg + \mathfrak{m}^3$ contains no sum of squares in A , which proves the initial claim. \square

As a consequence, Corollary 4.4 does not extend to curves with a non-isolated real singular point.

Corollary 4.6. *Let C be an affine curve over \mathbb{R} , and assume that C has a real singular point which is not an isolated point of $C(\mathbb{R})$. Then there exists a finitely generated quadratic module M in $\mathbb{R}[C]$ which is not a preordering, but for which $K = \mathcal{S}(M)$ is compact.*

Remark 4.7. On the other hand, there exist real curve singularities which are isolated and in which every quadratic module is a preordering. For example, if C is the curve $y^2 = x^2(x - 1)$, then every quadratic module M with compact associated set $K = \mathcal{S}(M)$ is a preordering. On the other hand, this fails for the curve $y^4 = x^2(x - 1)$.

Acknowledgments

Support by DFG travel grant KON 1823/2002 and by the European RAAG network HPRN-CT-2001-00271 is gratefully acknowledged. Part of this work was done while the author enjoyed a stay at MSRI Berkeley. He thanks the institute for the invitation and the very pleasant working conditions.

References

- [1] R. Berr, T. Wörmann, Positive polynomials on compact sets, *Manuscripta Math.* 104 (2001) 135–143.
- [2] J. Bochnak, M. Coste, M.-F. Roy, *Real Algebraic Geometry*, *Ergeb. Math. Grenzgeb.* (3), vol. 36, Springer-Verlag, Berlin, 1998.
- [3] J. Bochnak, J.-J. Risler, Le théorème des zéros pour les variétés analytiques réelles de dimension 2, *Ann. Sci. École Norm. Sup.* (4) 8 (1975) 353–364.
- [4] T. Jacobi, A representation theorem for certain partially ordered commutative rings, *Math. Z.* 237 (2001) 259–273.
- [5] T. Jacobi, A. Prestel, Distinguished representations of strictly positive polynomials, *J. Reine Angew. Math.* 532 (2001) 223–235.
- [6] M. Knebusch, C. Scheiderer, *Einführung in die reelle Algebra*, Vieweg, Wiesbaden, 1989.
- [7] S. Kuhlmann, M. Marshall, Positivity, sums of squares and the multi-dimensional moment problem, *Trans. Amer. Math. Soc.* 354 (2002) 4285–4301.

- [8] S. Kuhlmann, M. Marshall, N. Schwartz, Positivity, sums of squares and the multi-dimensional moment problem II, *Adv. Geometry*, in press.
- [9] M. Marshall, Representations of non-negative polynomials having finitely many zeros, preprint, 2004.
- [10] A. Prestel, C.N. Delzell, *Positive Polynomials*, Monogr. Math., Springer-Verlag, Berlin, 2001.
- [11] M. Putinar, Positive polynomials on compact semi-algebraic sets, *Indiana Univ. Math. J.* 42 (1993) 969–984.
- [12] C. Scheiderer, Sums of squares of regular functions on real algebraic varieties, *Trans. Amer. Math. Soc.* 352 (1999) 1039–1069.
- [13] C. Scheiderer, On sums of squares in local rings, *J. Reine Angew. Math.* 540 (2001) 205–227.
- [14] C. Scheiderer, Sums of squares on real algebraic curves, *Math. Z.* 245 (2003) 725–760.
- [15] C. Scheiderer, Positivity and sums of squares: A guide to some recent results, preprint, 2003, available at <http://www.ihp-raag.org/publications>.
- [16] M. Schweighofer, A criterion for membership in archimedean semirings, preprint, 2004.
- [17] K. Schmüdgen, The K -moment problem for compact semi-algebraic sets, *Math. Ann.* 289 (1991) 203–206.